TRUETRADE: A DECENTRALIZED MARKETPLACE WITH INTEGRATED ANONYMIZATION FUNCTION

Tyr Stephansen
tyrstephansen@gmail.com

Abstract: A decentralized marketplace cryptocurrency wherein nodes act as shops anonymously. An example implementation is given.

1. Introduction

It has become apparent that cryptocurrencies require integration with other decentralization efforts, such as anonymous marketplaces and mixing services. Elliptic curve cryptography is deemed essential in the implementation of such a scheme.

2. Elliptic Curve Cryptography

An elliptic curve is a plane curve over a finite field which consists of the points satisfying equation 1.

$$y^2 = x^3 + ax + b \qquad (1)$$

In ECC all parties must agree on all the elements defining the elliptic curve, that is, the domain parameters of the scheme. The field is defined by p in the prime case and the pair of m and f in the binary case. The elliptic curve is defined by the constants a and b used in its defining equation. Finally, the cyclic subgroup is defined by its generator G.

2. Implementation

A protocol based on one-time ring signatures allows users to achieve unconditional unlinkability. Unfortunately, ordinary types of cryptographic signatures permit to trace transactions to their respective senders and receivers. Our solution to this deficiency lies in using a different signature type than those currently used in electronic cash systems.

Using ECC it is possible to prove that an entity belongs to a certain group, a function that is essential to decentralized marketplaces. A typical transaction will proceed as follows:

Alice decides to spend an output, which was sent to the one-time public key. She needs extra, txOutNumber, and her account private key to recover her one-time private key.
When sending a transaction to Carol, Alice generates her extra value by random. She uses extra, txOutNumber and Carol's public key to get her output public key. In the input Alice hides the link to her output among the foreign keys. To prevent double-spending she also packs the key image, derived from her one-time private key.
Finally, Alice signs the transaction, using her one-time private key, all the public keys and the key image. She appends the resulting ring signature to the end of the transaction.

3. Generalization to anonymous marketplaces

The described anonymization mechanism will enable a cryptocurrency node to operate a fully automatic online shop anonymously.
An example of a complete implementation of this is given with the release of Kooliocoin.

4. Conclusion

An anonymous decentralized marketplace integrated into a cryptocurrency has been proposed. An example implementation is presented in an update of Kooliocoin[1].

[1] (https://bitcointalk.org/index.php?topic=686727.0)